Schneider Electric Security Notification

Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium

8 December 2020

Overview

Schneider Electric is aware of multiple vulnerabilities in its Modicon programmable automation controllers.

The Modicon Ethernet Programmable Automation products are controllers for industrial process and infrastructure.

Failure to apply the remediations provided below may risk a denial of service attack, which could result in making the device enter a non-recoverable fault state.

Affected Products & Versions

Product and Affected Versions	CVE
Modicon M580 CPUs – BMEx58xxxxx prior to version 3.20	CVE-2020-7537, CVE-2020-7542, CVE-2020-7543
Modicon M340 CPUs – BMX P34x prior to version 3.30	CVE-2020-7537, CVE-2020-7542, CVE-2020-7543
Modicon Premium CPUs all versions – TSXP574634, TSXP575634, TSXP576634	CVE-2020-7537, CVE-2020-7542
Modicon Quantum CPUs all versions – 140CPU65xxxxx	CVE-2020-7542

Vulnerability Details

CVE ID: **CVE-2020-7537**

CVSS v3.0 Base Score 7.5 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller.

Schneider Electric Security Notification

CVE ID: **CVE-2020-7542**

CVSS v3.0 Base Score 7.5 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a specially crafted Read request over Modbus is send to the controller.

CVE ID: **CVE-2020-7543**

CVSS v3.0 Base Score 7.5 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause a denial of service of the controller when a malformed Routing request over Modbus is send to the controller.

Remediation & Mitigations

Product and Affected Versions	Remediation/Mitigation
Modicon M580 CPUs - BMEx58xxxxx prior to version 3.20	These vulnerabilities are fixed in firmware version 3.20, available for all product references. Follow this link to find the right firmware file based on model used: https://www.se.com/ww/en/product-range/62098-modicon-m580/ *If customers choose not to apply the remediation provided above, they should immediately apply the Modicon M580 Mitigations provided below to reduce the risk of exploit.*
Modicon M340 CPUs – BMX P34x prior to version 3.30	These vulnerabilities are fixed in firmware version 3.30, available for all product references. Follow this link to find the right firmware file based on model used: https://www.se.com/ww/en/product-range/1468-modicon-m340/ *If customers choose not to apply the remediation provided above, they should immediately apply the Modicon M340 Mitigations provided below to reduce the risk of exploit.*
Modicon Premium CPUs all versions - TSXP574634, TSXP575634, TSXP576634	See Modicon Premium Mitigations below.

Modicon Quantum CPUs all versions - 140CPU65xxxxx	See Modicon Quantum Mitigations below.

Customers should use appropriate methodologies when upgrading their systems. We strongly recommend the use of back-ups and evaluating the impact of these upgrades in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric's Customer Care Center if you need assistance removing a patch.

Mitigations

Modicon M580:
To mitigate the risks associated to Modbus weaknesses, users should immediately:

- Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP

  Setup a secure communication according to the following guideline "Modicon Controllers Platform Cyber Security Reference Manual," in chapter "Setup secured communications": https://www.se.com/ww/en/download/document/EIO0000001999/

- Use a BMENOC module and follow the instructions to configure IPSEC feature as described in the guideline "Modicon M580 - BMENOC03.1 Ethernet Communications Module, Installation and Configuration Guide" in the chapter "Configuring IPSEC communications": https://www.se.com/ww/en/download/document/HRB62665/

Modicon M340:
To mitigate the risks associated to Modbus weaknesses, users should immediately:

- Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP
- Configure the Access Control List following the recommendations of the user manual "Modicon M340 for Ethernet Communications Modules and Processors User Manual" in chapter "Messaging Configuration Parameters": https://www.se.com/ww/en/download/document/31007131K01000/

Modicon Premium:
Schneider Electric's Modicon Premium controllers have reached their end of life and are no longer commercially available. They have been replaced by the Modicon M580 ePAC controller, our most current product offer. Customers should strongly consider migrating to the Modicon M580 ePAC. Please contact your local Schneider Electric technical support for more information.

To mitigate the risks associated to Modbus/ weaknesses, users should immediately:

- Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP
- Configure the Access Control List following the recommendations of the user manual "Premium and Atrium using EcoStruxure™ Control Expert - Ethernet Network Modules, User Manual" in chapters "Connection configuration parameters / TCP/IP Services Configuration Parameters / Connection Configuration Parameters": https://www.se.com/ww/en/download/document/35006192K01000/

Modicon Quantum:
Schneider Electric's Modicon Quantum controllers have reached their end of life and are no longer commercially available. They have been replaced by the Modicon M580 ePAC controller, our most current product offer. Customers should strongly consider migrating to the Modicon M580 ePAC. Please contact your local Schneider Electric technical support for more information.

To mitigate the risks associated to Modbus/ weaknesses, users should immediately:

- Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP
- Configure the Access Control List feature as mentioned in "Quantum using EcoStruxure™ Control Expert - TCP/IP Configuration, User Manual" in chapter "Software Settings for Ethernet Communication / Messaging / Quantum NOE Ethernet Messaging Configuration": https://www.se.com/ww/en/download/document/33002467K01000/

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the "Program" mode.

- Never connect programming software to any network other than the network for the devices that it is intended for.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow mobile devices that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and systems, and ensure that they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

For more information refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

Acknowledgements

Schneider Electric recognizes the following researchers for identifying and helping to coordinate a response to this vulnerability:

CVE	Researchers
CVE-2020-7537	Gao Jian (NSFOCUS) Daniel Lubel (OTORIO) Armis Security
CVE-2020-7542	Victor Fidalgo Villar (INCIBE - Spanish National Institute of Cybersecurity)
CVE-2020-7543	Gideon Guo

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, please contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

https://www.se.com/ww/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Schneider Electric Security Notification

THIS NOTIFICATION DOCUMENT, THE INFORMATION CONTAINED HEREIN, AND ANY MATERIALS LINKED FROM IT (COLLECTIVELY, THIS "NOTIFICATION") ARE INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN "AS-IS" BASIS WITHOUT WARRANTY OR GUARANTEE OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES RELATING TO THIS NOTIFICATION, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY RESULT FROM YOUR USE OF THIS NOTIFICATION. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 *8 December 2020*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2020.12.06 14:25:08 -05'00'